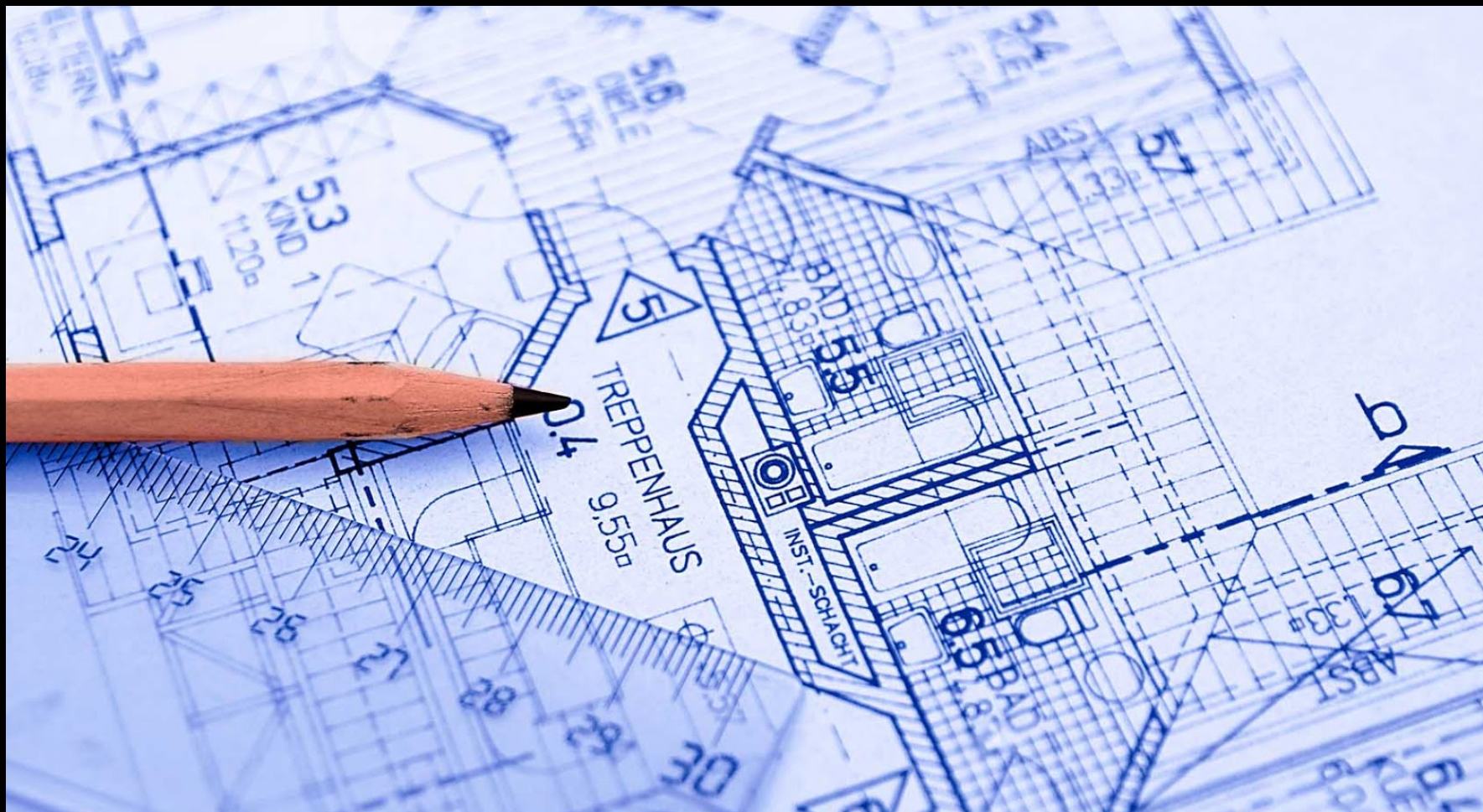


Practical Steps Taken to Reboot Vulnerability Management for Modern IT and Mature Business

Brian Canaday
IT Security Analyst/Engineer
CSAA, Insurance Group a AAA Insurer

Key Talking Points

- A Three-Phase Approach to Meeting our Vulnerability Management Goals with Qualys
- Scan Configurations & Schedule Tuning
- Cloud Agent Configuration & Testing with Application Teams





1. What
2. Build
3. Confi

Configure Scan Performance Settings Turn help tips: On | Off

Settings

Select a performance level or customize performance settings for network analysis.

☒ Enable parallel scaling for Scanner Appliances

Overall Performance Custom ▼

Hosts to Scan in Parallel

External Scanners 30 ▼

Scanner Appliances 50 ▼

Processes to Run in Parallel (per Host)

Total Processes 10 ▼

HTTP Processes 10 ▼

Packet Delay

Packet (Burst) Delay Long ▼

Port Scanning and Host Discovery

Intensity Normal ▼

OK Cancel

Document
ces



1. Plan and
 2. Identify T
 3. Identify T
 4. Test, Tun
 5. Deploy in
 6. Deploy in
- With all d

Configuration Profile Edit

Turn help tips: On | Off

Edit Mode

- General Info
- Blackout Windows
- Performance**
- Assign Hosts
- VM Scan Interval
- PC Scan Interval
- IOC

Configure Agent Performance

These settings govern how an agent behaves, from how often it checks into the Qualys Cloud platform, to how often it checks the host for changes. It also includes performance settings that control CPU and network utilization.

Performance
Select one of the performance levels below. Keep the default settings or customize them. **Customize** ☒

Based On:

Set Parameters

Agent Status Interval* Push interval in seconds to update system with Agent's status	<input type="text" value="2700"/> sec(900 - 7200)
Delta Upload Interval* Interval an agent attempts to upload detected changes	<input type="text" value="10"/> sec(1 - 1800)
Chunk sizes for file fragment uploads* This is the upload block size, and combined with the above Network throttle Tx, determines network utilization	<input type="text" value="1024"/> KB(64 - 10240)
Upgrade Reattempt Interval* Interval an agent will retry applying a new upgrade to itself	<input type="text" value="300"/> sec(180 or more)
Logging level for agent* This is the logging level for the agent.	<input type="text" value="Error"/>

WINDOWS SPECIFIC PARAMETERS (versions 1.5 and above)

CPU Limit* Defines the percentage limit of the processor core(s) used by the agent. Lower percentages reduces CPU utilization at the expense of longer execution times.	<input type="text" value="5"/> %(2 - 100)
---	---

ing the Agent
hose to Work
the Agent.

PHASE 3

Vulnerability Management

Dashboard Search **Scans** Reports Remediation Assets KnowledgeBase Users

Scans Scans Maps Schedules Appliances Option Profiles Authentication Search Lists Setup

Actions (1) New Search Filters Active Tasks

Type	Title	Targets	Scanner	Assigned User	Next Launch
	Glendale Call Center (GCC) - Daily	Asset Tags Included	All Scanners in TagSet	Service Account	09/13/2018 at 10:00:00 AM
	Glendale Call Center (GCC) - Cloud Agent - Remote Only Vulnerabi	Asset Tags Included	All Scanners in TagSet	Service Account	09/13/2018 at 10:00:00 AM

Glendale Call Center (GCC) - Cloud Agent - Remote Only Vulnerabi

Type: Scan

Target Asset Groups: -

Target Asset Tags: Included (all): Cloud Agent Glendale Call Center... Excluded (all): No_Scan Network Dev...

Target Hosts: -

Excluded IPs: -

Next launch: 09/13/2018 at 10:00:00 AM (GMT-0700)
09/13/2018 at 10:00:00 AM (GMT-0700)

Start: 08/23/2018 at 10:00

Time Zone: (GMT-07:00) United States, Arizona (Mo

Daylight Saving Time: Off

Duration: -

Resume: -

Occurrence: Every day
No end date

Option Profile: Qualys Cloud Agent Remote QIDs

Scanner Appliance: All Scanners in TagSet

Owner: Service Account (csaan3sa)

Created: 07/09/2018 at 02:40:45 PM (GMT-0700)

Modified By: Brian Canaday (csaan3bc)

Modified: 09/04/2018 at 02:29:22 PM (GMT-0700)

Edit Scheduled Vulnerability Scan

Turn help tips: On | Off Launch Help

Task Title >

Target Hosts >

Scheduling >

Notifications >

Schedule Status >

Run History >

☐ Assets

☒ Tags

☐ Scan agent hosts in my target

☐ Use IP Network Range Tags
Choose from tags defined with IP address rules. This will allow you to scan the entire IP range(s) in each selected tag.

Include hosts that have All of the tags below. Add Tag

Glendale Call Cen... Cloud Agent X

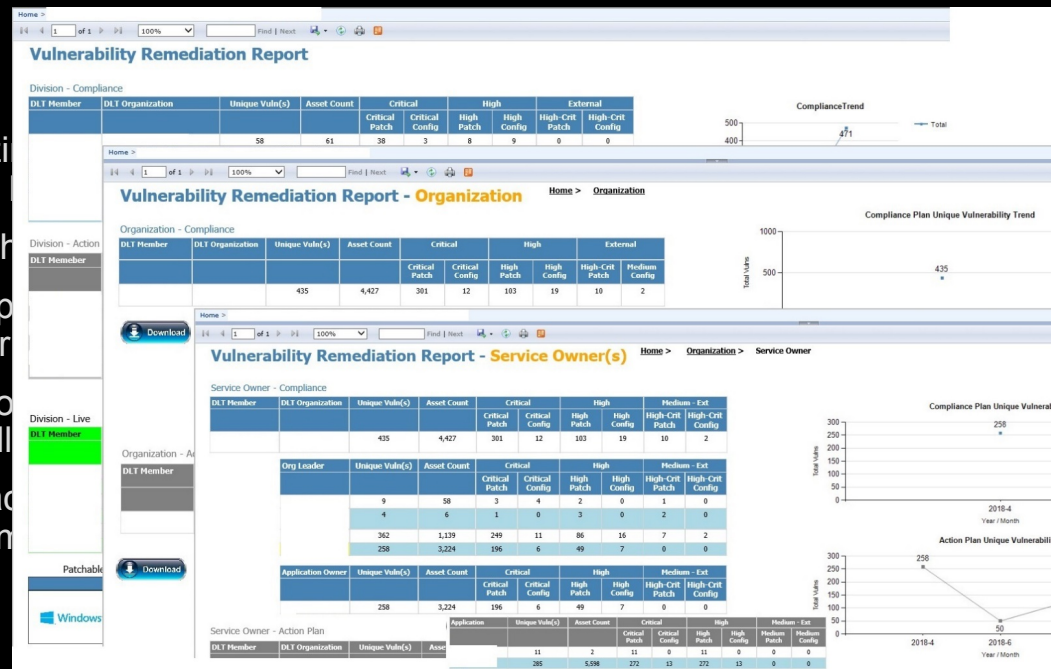
Do not include hosts that have All of the tags below. Add Tag

No_Scan Network D... X

Cancel Save

Reporting - Better Data, Better Results

- Utilize Four
- With The
- 1. App
- 2. Our
- 2. Sho
- 3. Drill
- 3. Trac
- San



Every

Only Items

Ability to

aging the

Outcomes

- With cleaner more relevant data we can detect changes in our environment sooner
- With faster results and less impact on the systems the Qualys Cloud Agent has quickly become the one security agent our Operations Teams depend on and expect immediate remediation of any agent not reporting in
- By leveraging the API from Qualys and our CMDB we use a custom reporting solution where we rollup under the VP for each area and the leaders under them

Questions

